Amendments to the Claims

The following listing of the claims will replace all prior versions, and listings, of claims in the application. Inserted material is underlined and deleted material is shown in strikethrough to show the changes made.

1. (Currently Amended) A method for regulating access to a ~~nonvolatile digital~~ storage ~~contained~~ within an audiovisual player device, the device configured for executing instructions in a Turing-complete interpreter, the device further configured to render content for playback, said method comprising:

(a) receiving a request from ~~said~~ a first set of instructions being executed, wherein said request specifies:

(i) a first portion of said storage for which access is requested, the first portion of the storage for enabling rendering of the content by the device, and

(ii) a plurality of additional executable instructions;

(b) applying a cryptographic hash function to said additional executable instructions to obtain a hash value;

(c) authenticating said hash value; ~~and~~

(d) provided that said authentication is successful, enabling access by said first set of instructions being executed to said requested first portion of said storage while executing said additional executable instructions; and

(e) if the authentication is not successful, inhibiting at least one of

(i) the rendering of the content, and

(ii) execution of at least one feature associated with the content.

2. (Currently Amended) The method of claim 1 wherein said step of authenticating comprises comparing said hash value with a hash value stored in said ~~nonvolatile~~ storage.

3. (Currently Amended) The method of claim 1 wherein said step of authenticating comprises verifying a digital signature provided by said first set of instructions being executed.

4. (Currently Amended) The method of claim 1 wherein said request includes a pointer to said additional executable instructions in memory accessible by said first set of instructions being executed ~~and contained in said device~~.

5. (Currently Amended) A ~~digital optical disc~~ storage medium containing encrypted audiovisual content for playback on any of a plurality of device architectures, ~~said digital optical disc~~ the storage medium comprising program logic configured to:

(a) identify at least one characteristic of a device executing said program logic;

(b) use said at least one characteristic to determine which, if any, of a plurality of security weaknesses are present in said ~~executing~~ device;

(c) when said determination indicates a suspected weakness,

(i) select at least one of a plurality of software countermeasures, wherein said selected countermeasure corresponds to said suspected weakness and is compatible with said ~~executing~~ device;

(ii) mitigate said suspected weakness by directing said ~~executing~~ device to invoke said selected countermeasure; and

(iii) decode said encrypted audiovisual content, wherein said decoding includes a result produced by successful operation of said countermeasure logic; and

(d) when said determination does not indicate a suspected weakness, decode said audiovisual content by using at least one decryption key derived by using at least one cryptographic key associated with said ~~executing~~ device.

6. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is configured to execute in an interpreter common to ~~said~~ a plurality of device architectures, and at least a portion of said selected countermeasure is configured to be executed directly as native code on a microprocessor associated with said ~~executing~~ device.

7. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 ~~wherein said digital optical disc medium~~ further ~~includes~~ comprising a digital signature authenticating said native code portion.

Claims 8-10 (canceled).

11. (Currently Amended) An automated method for determining whether to allow a portion of software ~~stored in a computer readable memory~~ to access a portion of a ~~nonvolatile~~ memory within an audiovisual player device, the method comprising:

(a) receiving a reference to said portion of software;

(b) computing a cryptographic hash of said software portion;

(c) comparing said computed cryptographic hash with a value stored in said ~~nonvolatile~~ memory,

(d) when said computed cryptographic hash matches said stored value,

(i) allowing said software portion to access said portion of the ~~nonvolatile~~ memory ~~portion~~ , the portion of the memory for enabling rendering of the content by the device, and

(ii) permitting execution of at least one feature associated with the content; and

(e) when said computed cryptographic hash does not match said stored value,

not allowing said software portion to access said nonvolatile memory and inhibiting at least one of

(i) the rendering of the content or

(ii) execution of at least one feature associated with the content.

12. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is further adapted to cryptographically authenticate at least one of manufacturer, model, and version of the device executing said program logic.

13. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is adapted to verify as at least one characteristic of the device whether the device can perform block cipher operations using a key characteristic of at least one of manufacturer, model, and version of the device.

14. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is adapted to verify as at least one characteristic whether unauthorized firmware is present on the device.

15. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is configured to access a server over a network and to receive from the server data representing at least one of code configured to identify a new characteristic, code implementing a countermeasure, revocation status, payment information associated with content, download of bonus content, and download of advertisement.

16. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is configured to identify a characteristic by searching a portion of memory of the device.

17. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is configured to identify a characteristic by accessing non-volatile storage of the device.

18. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 5 wherein said program logic is further configured to make video playable by applying modifications to a video data stream.

19. (Currently Amended) The ~~digital optical disc~~ storage medium of claim 18 wherein said program logic is further configured to change, when applying said modifications, audiovisual content to embed forensic information associated with playback environment.

Please add the following new claims.

20. (New) The method of claim 1, wherein the audiovisual player device includes a removable disk player to receive the content, and wherein the Turing-complete interpreter:

receives the first set of instructions from the disk player, and

executes the first set of instructions in the audiovisual player device, such that the request originates from disk.

21. (New) The method of claim 1, wherein the audiovisual player device includes a network connection to receive the content, and wherein the Turing-complete interpreter:

receives the first set of instructions from the network, and

executes the first set of instructions in the audiovisual player device, such that the request originates from a network source.

22. (New) The method of claim 1, wherein:

the portion of the storage includes a slot reserved for at least one program title;

the method further comprising determining whether new content seeks access to a new slot or to an existing slot.

23. (New) The method of claim 22, wherein enabling access includes granting access to one of the existing slot and the new slot.

24. (New) The method of claim 1, wherein enabling access includes storing at least one of: (i) information regarding payment associated with the content; (ii) a counter value; (iii) a spending limit; (iv) permission to access content special features; (v) pay-per-view history; (vi) a privilege level; or (vii) pricing discount information.

25. (New) The method of claim 1, wherein enabling access includes storing at least one of: (i) information about a security policy; (ii) security vulnerability fix code; (iii) a cryptographic key; (iv) security check data; or (v) a digital signature.

26. (New) The method of claim 11, wherein the audiovisual player device includes a removable disk player to receive the content, and wherein the device retrieves the software from the disk player and executes the software in the audiovisual player device, such that the reference originates from disk.

27. (New) The method of claim 26, wherein the audiovisual player device includes a network connection, and wherein allowing the software portion to access the memory portion includes writing a value arising from a network source into the memory portion.

28. (New) The method of claim 27, wherein:

the memory portion includes a slot reserved for at least one program title;

the method further comprising determining whether new content seeks access to a new slot or to an existing slot; and

allowing the software portion to access the memory portion includes granting access to the existing slot.

29. (New) The method of claim 11, wherein inhibiting at least one of the rendering of the content or execution of at least one feature associated with the content includes taking an action selected from a group of:

inhibiting access to bonus content, halting playback, reporting an error, requiring additional authentication, requiring a player upgrade, refusing to decode the end of a movie, disabling bonus features, and playing at reduced resolution.